

# **An Analytical Study of the Jurisprudential Development of Right to Privacy and Its Working on International Standards: A Comparative View**

**Mr. Sandeep Shravan Sawalkar\***

## **Introduction**

य आस्तेयश्चरतिपश्यतिनोजनः  
तेषांसंहन्मोअक्षाणियथेदंहनेतथा

(One must build a house in such a manner as it protects from the inmates and the passer-by shall not see the inmates nor the inmates not see them). An ancient civilization has made a distinction between the “Outer” and the ‘Inner’ man, between the spirit and the body, between the mystical and the material, between the sacred and the blasphemous, between the realm of God and the realm of Caesar, between the Ecclesiastical and the State, between society and solitude, between public and private, by whatever name it may be called, the thought of “private space in which individuals may become and remain themselves” cannot be avoided.<sup>2</sup>

The need for the right to privacy is inherent in human nature as it allows individuals to establish personal boundaries and prevent others from intruding into their personal space. This fundamental right serves as a means of safeguarding individual autonomy and control over one’s personal information and activities. Both Oriental and Occidental civilizations provide enough evidence to support this view. Animal behaviour and social organisation studies imply that man’s demand for privacy may have its beginnings in animals only and that animals & mankind both share some fundamental strategies for expressing their privacy among their kind.<sup>3</sup> The concept of privacy has been present since ancient times, as evidenced by its mention in texts from both the Vedic and Biblical eras. This demonstrates that the need for individuals to maintain personal boundaries and protect their private lives has been recognized and valued throughout human history. Disturbing a meditating sage has long been considered a sin or a wrong of the greatest degree in Indian civilization, dating back to Vedic times. In Indian mythology, there is a tale where Lord Shiva, who was in a state of deep meditation known as samadhi, was

---

\* Assistant Professor, Chembur Karnataka College of Law, University of Mumbai, Mumbai and Ph.D Research Scholar at Maharashtra National Law University, Mumbai

<sup>1</sup> Rigveda, Mandal 7, Sukta 55, Hymn 6

<sup>2</sup> *Shyambabu Verma v State of Madhya Pradesh*, 1997 (1) MPLJ 504

<sup>3</sup> Westin A, ‘Privacy And Freedom’ (1968) 25 Washington and Lee Law Review 166 <https://scholarlycommons.law.wlu.edu/wlulr/vol25/iss1/20> accessed on 10th February 2023

disturbed by Kamdeva, the god of love and desire. As a consequence, Kamdeva was punished and burnt by Lord Shiva's third eye.<sup>4</sup> Similarly, the Bible tells the story of Adam and Eve, who became aware of their nakedness and fashioned aprons from fig leaves to cover themselves. Both of these examples illustrate the human need for privacy and the desire to control one's personal space and information.<sup>5</sup>

### **International Approaches**

Privacy is preserved in several international legal documents such as The Universal Declaration of Human Rights (UDHR)<sup>6</sup>, the International Covenant on Civil and Political Rights (ICCPR)<sup>7</sup> contains an almost identical provision of UDHR, The European Convention on Human Rights (ECHR)<sup>8</sup>, and The American Convention on Human Rights<sup>9</sup> and so on. However, neither of these documents defines privacy. It's a challenging task to define privacy as it encompasses various dimensions and has different meanings depending on the context in which it is applied. The term 'privacy' is complex and multidimensional, making it difficult to provide a single, concise definition that accurately captures its essence.<sup>10</sup> 'What is privacy?' is a question that has confounded legal scholars, philosophers, sociologists, and psychologists for centuries.<sup>11</sup> Many of them have despaired of arriving at a satisfactory definition of the concept of privacy.<sup>12</sup> As a concept, privacy has been accused of being 'Vagabondize and evanescent',<sup>13</sup> 'equivocal and notoriously elastic',<sup>14</sup> 'it is engorged with numerous and distinct meanings',<sup>15</sup> 'extremely subjective',<sup>16</sup> 'culture-specific',<sup>17</sup> and operating 'in a wide array of context'.<sup>18</sup>

<sup>4</sup> Kalidas, *Kumarsambhavam*, 3/17.

<sup>5</sup> The Holy Bible American Standard Version (1929), Genesis 3:7.

<sup>6</sup> The Universal Declaration of Human Rights 1948, art 12.

<sup>7</sup> International Covenant on Civil and Political Rights ICCPR 1966, art 17.

<sup>8</sup> The European Convention on Human Rights 1953, art 8(1).

<sup>9</sup> The American Convention on Human Rights 1978, art 11(2).

<sup>10</sup> W Beaney, 'The Right to Privacy and American Law' (1996) 31 *Law & Contemporary Problems* 253, 255.

<sup>11</sup> AD Moore, *Privacy Rights: Moral and Legal Foundations* (University Park PA, The Pennsylvania State University Press, 2010) 11.

<sup>12</sup> C Raab and CJ Bennett, 'Taking the Measure of Privacy: Can Data Protection Be Evaluated?' (1996) 62 *International Review of Administrative Science* 535.

<sup>13</sup> AR Miller, *The Assault on Privacy: Computer, Data Banks, and Dossier* (University of Michigan Press, 1973).

<sup>14</sup> H Delany and E Carolan, *The Right to Privacy: A Doctrinal and Comparative Analysis* (Thompson Round Hall, Ireland, 2008).

<sup>15</sup> RC Post, 'Three Concepts of Privacy' (2000) 89 *Georgetown Law Journal* 2087.

<sup>16</sup> CJ Bennett and C Raab (eds), *The Governance of Privacy: Policy Instruments in a Global Perspective* (MIT Press, US, 2006) 8.

<sup>17</sup> Supra n.11, p 6.

<sup>18</sup> Be Vier, 'Information about Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection' (1995) 4 *William and Mary Bill of Rights Journal* 455, 458.

Although privacy is conceptually difficult, this does not diminish its importance.<sup>19</sup> For a significant period of time, the right to privacy has been considered the most valuable right that civilized individuals possess. This illustrates the critical importance placed on preserving personal boundaries and safeguarding an individual's right to control their personal information and activities without unwanted intrusion.<sup>20</sup> and its importance has rarely been called into question.<sup>21</sup> Academic literature has argued for the value of privacy through deontological and consequentialist theories.<sup>22</sup> Deontological theories hold that privacy is an inherent value that is linked to an individual's humanity, autonomy, and personhood. In this sense, the invasion of privacy is seen as a violation of these values and a threat to an individual's dignity.<sup>23</sup> In this context, privacy is connected to human dignity, autonomy, and personhood, and its invasion constitutes an affront to these values.<sup>24</sup> In contrast, consequentialist theories focus on the positive outcomes that can be derived from the protection of privacy, both for individuals and for society as a whole. These theories stress the importance of privacy in promoting various goods and highlight the potential negative consequences that can arise from its violation.<sup>25</sup> In the view of privacy, it acts as a safeguard against oppression from government and totalitarian regimes.<sup>26</sup> In this vein, the argument normally goes that privacy has value because it limits the oppression of the forces of 'despotic regimes'.<sup>27</sup>

<sup>19</sup> *Olmstead vUnited States*, 277 US 438, 478 (1928).

<sup>20</sup> Some Scholars have questioned the inherent value of privacy. A Etzioni, *The Limits of Privacy* (Basic Books, New York, 1999); RA Posner, *The Economics of Justice* (Harvard University Press, 1983) 229; G Sartor, *Privacy, Reputation, and Trust: Some Implications for Data Protection* (European University Institute, EUI Working Papers, Law No 2006/04, 7).

<sup>21</sup> C Hunt, 'Conceptualizing Privacy and Elucidating its Importance: Foundational Considerations for the Development of Canada's Fledgling Privacy Tort' (2011) 167 Queen's Law Journal 202.

<sup>22</sup> Id. at p. 639.

<sup>23</sup> Ibid.

<sup>24</sup> Id. at p. 640

<sup>25</sup> A D Moore, 'Privacy, Speech, and Values: What we have no Business Knowing' (2016) 41 Ethics & Information Technology, 43.

<sup>26</sup> Ibid.

<sup>27</sup> SD Warren and LD Brandeis, 'Right to Privacy' IV Harvard Law Review, (1890) 193-220

Over time, a variety of definitions have been proposed to capture the complex nature of privacy. One influential definition is the concept of privacy as ‘the right to be let alone,’ which was first introduced in the seminal article ‘The Right to Privacy’ by Samuel Warren and Louis Brandeis. Their work was groundbreaking in its recognition of the importance of preserving personal boundaries and the need to protect individuals from unwanted intrusion.<sup>28</sup> In this path-breaking work,<sup>29</sup> Warren and Brandeis contended that-

“Every individual has the right to determine, ordinarily, to what extent his thoughts, sentiments, and emotions may be disclosed to others under the common law.”<sup>30</sup> Privacy is also defined as the “Individuals have the right to select how much knowledge the public at large shall have about their personal thoughts, feelings, private affairs, and private doings.”<sup>31</sup> There are various interpretations of this definition, called the restricted admission to one’s self-perception of privacy,<sup>32</sup> that has been developed by several legal scholars.<sup>33</sup> In addition, privacy has also been equated with the ‘concealment of information’<sup>34</sup> from others. An alternative theory views privacy as safeguarding an individual’s interests in becoming, remaining, and becoming who he or she is.<sup>35</sup> Moreover, intimacy has also been conceived of as a form of privacy. Thus, privacy is “the state of a person who has control over decisions regarding matters that have meaning and value due to their love, care, or liking”.<sup>36</sup> In the minds of some authors, private information is construed as an individual’s control. According to Alan Westin, privacy is “an individual, group, or institution’s right to decide when, how, and to what extent information about them is shared with others.”<sup>37</sup>

Moreover, privacy is often understood to be protecting what is deemed ‘private’ rather than ‘public’.<sup>38</sup> As a result, the distinction between ‘private’ and ‘public’ spheres is often made in this respect,<sup>39</sup> ‘publicity’ and ‘privacy’.<sup>40</sup> In this

<sup>28</sup> H Kalven, ‘Privacy in Tort Law - were Warren and Brandeis Wrong?’ (1966) *Law and Contemporary Problems* 326-327.

<sup>29</sup> Supran. 23, p 205.

<sup>30</sup> E Godkin, ‘The Rights of the Citizen to His Own Reputation’ (1890) *Scribner’s Magazine* 58-65.

<sup>31</sup> Supran. 15, p 18.

<sup>32</sup> S Bok, *Secrets: On the Ethics of Concealment and Revelation* (Vintage Books, US, 1989) 10.

<sup>33</sup> R Posner (ed), *Economic Analysis of Law* (Aspen Books, US, 1998) 46.

<sup>34</sup> JH Reiman, ‘Privacy, Intimacy, and Personhood’ (1976) 26 *Philosophy and Public Affairs*.

<sup>35</sup> JC Inness, *Privacy, Intimacy and Isolation* (Oxford University Press, 1996) 56.

<sup>36</sup> A Westin, *Privacy and Freedom* (The Bodley Head, London, 1970) 142.

<sup>37</sup> P de Hert, ‘The Case of Anonymity in Western Political Philosophy – Benjamin Constant’s Refutation of Republic and Utilitarian Arguments Against Anonymity’ in Nicoll et al (eds), *Digital Anonymity and The Law: Tensions and Dimensions* (TMC Asser Press, Hague, 2003) 47-52.

<sup>38</sup> J Habermas, *The Structural Transformation of the Public Sphere – An Inquiry into a Category of Bourgeois Society*, (Polity Press, UK, 1992).

<sup>39</sup> Ibid.

<sup>40</sup> Ibid.

sense, privacy is sometimes viewed as, ‘suspicious’<sup>41</sup> and ‘socially detrimental’,<sup>42</sup> since it encourages an ‘escape from society’.<sup>43</sup> The philosophers and legal scholars<sup>44</sup> trace this approach to privacy back to ancient Greece and Rome, where privacy was viewed as a negative concept since citizen life meant active participation in the polis. The republican philosopher Rousseau took up this theory further, private interests are viewed as a danger to the government and the demise of the state<sup>45</sup>. Whereas, Hannah Arendt heavily criticised a private life,<sup>46</sup> arguing that in ancient Greece, privacy meant ‘being deprived of something’.<sup>47</sup>

In contrast to the larger ‘society’,<sup>48</sup> privacy is perceived as an individual’s right in the context of private and public life.<sup>49</sup> As a result, this perspective overlooks the ‘broader societal relevance of privacy’,<sup>50</sup> since it views it as a right that only serves individuals. In Regan’s opinion, it is essential to accept that privacy has more value than simply preserving an individual’s dignity or fostering personal relationships. In practice, Privacy promotes ‘not just private but also public interests’,

Enormous apprehensions are already dominant concerning the infringement of individuals’ data and information. Individuals’ privacy refers to their ability to control how and where personal information is collected, used, and discovered. An individual’s personal information is made up of a variety of details, including interests, habits, and activities, family information, education, communications (including emails and telecommunications), medical, financial information, and many other things. Further, the revolution in technology has brought about a whole new set of issues with regard to data security and privacy rights. Modern technologies make it easy to access and transmit personal data. The prediction made by the Forrester Research Institute in 2019 indicated that as much as 2 million data of customer information has been leaked which raises customer privacy concerns.<sup>53</sup>

<sup>41</sup> Supra n. 15, p 80.

<sup>42</sup> Ibid.

<sup>43</sup> J Baily, ‘From Public to Private: The Development of the Concept of the Private’, 69, Social Research: An International Quarterly (2002).

<sup>44</sup> J Rousseau, *De Contract Social*(Swan Sonnenschein& Co, London, 1762) 365.

<sup>45</sup> H Arendt, *The Human Condition* 38 (University of Chicago Press, 1998).

<sup>46</sup> Ibid.

<sup>47</sup> RF Hixson, Privacy in Public Society: Human Rights in Conflict 212 (New York, Oxford University Press, 1987).

<sup>48</sup> Supra n. 15, p 89.

<sup>49</sup> PM Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* 213 (Chapel Hill, University of North Carolina Press, 1995).

<sup>50</sup> Id. at 321.

<sup>51</sup> Supra n. 15, pp 92-93.

<sup>52</sup> Forrester Research, ‘The Security Snapshot: Data Privacy - The Biggest Concern of the New Decade’ (As visited on December 27, 2019) <https://www.forrester.com/blogs/the-security-snapshot-data-privacy-the-biggest-concern-of-the-new-decade/>.

<sup>53</sup> The Constitution of the State of California (1849), Article I, Section 1.

## Right to Privacy from Developed to Third World Countries

### A. Developed Countries

#### United States

Although the concept of “privacy” may not be explicitly mentioned in the United States Constitution, the Supreme Court has established its constitutional significance through the due process clause and various Constitutional Amendments. However, it is important to note that the Supreme Court has not issued a comprehensive ruling affirming an all-encompassing constitutional right to privacy, as some legal scholars had predicted in the 1960s. The Constitution has not been officially modified in this regard, and there is no current agenda or active discussion regarding the addition of a specific federal constitutional right to privacy. It should be highlighted that, unlike the situation in certain states, U.S. citizens do not currently possess a distinct federal constitutional right to privacy.

collective, and societal interests.<sup>51</sup> Therefore, it is a public good because it protects individuals ‘for the benefit of society’.<sup>52</sup>

The California Constitution of 1972 includes an amendment that explicitly recognizes the right to privacy for its residents.<sup>54</sup> This constitutional provision enables individuals to assert their right to privacy not only against the government but also against private entities. While there may be challenges and costs associated with effectively pursuing privacy claims in court, it is crucial to revitalize these claims in Canada and other common law countries as a concrete safeguard for protecting individual privacy rights.<sup>55</sup>

The recognition of the right to privacy by the United States courts holds great significance as it provides insight into the circumstances under which privacy claims are more likely to be considered. Although the federal court acknowledged the rights to privacy since the late 19th century,<sup>56</sup> it was Justice Douglas who formalized the court’s decision by asserting the existence of a right to privacy against the state even before the Bill of Rights.<sup>57</sup> Douglas argued that “numerous amendments to the Constitution indirectly but clearly enshrined a series of safeguards for privacy”.<sup>58</sup> A notable case highlighting privacy is the *Griswold* decision, where the

---

<sup>54</sup> W.F.Pratt, *Privacy in Britain*(Bucknell University Press, 1979).

<sup>55</sup> Beaney, W.M., *The Constitutional Right to Privacy in the Supreme Court*, 212-251 (University of Chicago Press, 1962).

<sup>56</sup> Schwartz, B., ‘The Unpublished Opinions of the Warren Court’, 227-239 (The University of Chicago Law Review, 1986).

<sup>57</sup> *Griswold v. Connecticut*, 381 U.S. 482-86 (1965).

<sup>58</sup> Id., atp 497-80.

Supreme Court noted the absurdity of Connecticut's law, which made it illegal for anyone, including married couples, to use contraception. Physicians and family planning centres faced criminal charges for providing birth control information to their patients.<sup>59</sup> By overturning this statute, the Court effectively established a "right to marital privacy," which has since evolved into a significant right of intimate association.<sup>60</sup>

The Supreme Court reached a significant milestone in 1973 by laying the foundation for the constitutional right to privacy.<sup>61</sup> This was exemplified in a case where the right of a woman to make a decision regarding abortion served as the platform for asserting the right to privacy. The majority of the court declared that the right to privacy encompasses a woman's choice to terminate her pregnancy.<sup>62</sup> However, it should be noted that the Supreme Court also emphasized that a woman's right to privacy in reproductive choices is not absolute and must be weighed against state interests in regulating abortion. This reflects the common balancing test applied by courts when privacy claims are raised.<sup>63</sup> It is worth mentioning that courts typically prioritize the right to privacy in cases involving close relationships rather than situations where an individual seeks to establish privacy rights against the state or conceal potential wrongdoing.<sup>64</sup>

There is a gap in the right to privacy in USA is that the legal framework surrounding the collection of Cell-site location information CSLI<sup>65</sup> is not well defined. In 2012, the Supreme Court of the United States heard a case, *United States v Jones*<sup>66</sup>, that dealt with the use of GPS tracking devices on vehicles. In this case, the Court held that "the use of a GPS tracking device constituted a search under the 4<sup>th</sup> Amendment and required a warrant". However, the Court did not address the use of CSLI. The following year, in 2013, the Supreme Court heard another case, *United States v Carpenter*<sup>67</sup> that dealt specifically with the collection of CSLI. In Carpenter, the Court held that the collection of CSLI without a warrant violated the Fourth Amendment. The Court recognized that CSLI could reveal sensitive information about an individual's private life and held that this information was subject to the protections of the 4<sup>th</sup> Amendment.

<sup>59</sup>Bork, R.H., 'The Tempting of America: The Political Seduction of The Law', 95-100, 110-126 (BYU Law Review, J. Reuben Clark Law School, 1990).

<sup>60</sup>*Roe v Wade*, 410 U.S. 113 (1973).

<sup>61</sup>*Id* at 153.

<sup>62</sup>*Ibid.*

<sup>63</sup>*Hudson v Palmer*, 468 U.S. 517, 526 (1984).

<sup>64</sup> CSLI is data generated by mobile phones that indicates the location of the device at a given time. This information is collected by cellular service providers as part of their normal operations. Law enforcement agencies can obtain this information from service providers as part of an investigation. The collection of CSLI has been the subject of much debate in recent years due to its potential impact on the right to privacy.

<sup>65</sup> [2012] 565 U.S. 400.

<sup>66</sup> [2018] 585 U.S. 786.

<sup>67</sup> [2019] 588 U.S. 63.

The Carpenter ruling raised the unresolved issue of the extent to which law enforcement agencies can access information without a warrant. In a later case, *United States v Davis*<sup>68</sup>, the Court determined that historical cell-site data older than six months does not require a warrant for law enforcement to obtain. This decision has faced substantial criticism, as it permits law enforcement agencies to gather substantial information regarding an individual's whereabouts without the need for a warrant.

The utilization of CSLI by law enforcement agencies represents a notable loophole in the realm of privacy rights within the United States. While the Supreme Court acknowledges that CSLI is subject to Fourth Amendment protections, the legal framework governing its collection lacks clarity. The Davis ruling has received criticism for permitting law enforcement agencies to access substantial amounts of information without obtaining a warrant. As technology advances, it becomes imperative to establish a clear and updated legal framework that addresses the collection of CSLI, ensuring robust protection of the right to privacy.

### **Canada**

The Canadian Charter of Rights and Freedoms establishes the privacy rights of individuals in Canada. Similar to the United States Constitution, the Charter does not explicitly mention specific privacy protection, but it incorporates extensive safeguards within clauses that "protect life, liberty, or the safety of individuals"<sup>69</sup> as well as "against unreasonable searches and seizures"<sup>70</sup>. In contrast to the United States Supreme Court, the Supreme Court of Canada has developed a comprehensive and well-defined body of jurisprudence that interprets the right to privacy in a broad and purposeful manner. To further enhance privacy protections, Canada has enacted legislation such as the Privacy Act, Personal Information Protection Act, and Electronic Documents Act.

The Supreme Court of Canada, drawing inspiration from the decision of the United States Supreme Court,<sup>71</sup> granted authorization to the Investigation Department to conduct searches and seizures.<sup>72</sup> Additionally, the Court emphasized that the limitation imposed by Section 8 of the Charter, which safeguards against unreasonable search and seizure, requires an assessment of whether, in a particular situation, the public's interest in being free from government intrusion should yield to the government's interest in intruding on an individual's privacy to further its objectives, particularly in the realm of law enforcement.<sup>73</sup>

---

<sup>68</sup> The Constitution of Canada, Section 7.

<sup>69</sup> The Constitution of Canada, Section 8.

<sup>70</sup> *Katz v the US*, 389 U.S. 347 (1967)

<sup>71</sup> *Hunter et al v Southam, Inc*, [1984] 2 S.C.R. 145

<sup>72</sup> Ibid.

<sup>73</sup> *R v. Brandon Roy Dymont*, [1988] 2 S.C.R. 417

The Canadian Supreme Court was presented with a case involving a police officer who obtained a patient's blood sample, which had been collected by a doctor for medical purposes. One of the issues addressed was whether this action violated Section 8 of the Charter. In their ruling,<sup>74</sup> it was expressed that utilizing an individual's body without their consent to gather information about them undermines the inherent privacy necessary for safeguarding their human dignity.<sup>75</sup> The court also determined that while a patient may be considered to have implicitly given consent for a sample to be taken for medical purposes, they still maintain the expectation that their privacy rights will be upheld concerning the handling and usage of the sample. In other words, while there may be an understanding that the sample can be taken for medical reasons, the patient's privacy interest in the sample remains intact and should be respected.<sup>76</sup>

In another case, where the court deliberated on the legality of a warrantless perimeter examination leading to the discovery of marijuana plants. The majority opinion concluded that the examination violated Section 8 of the Charter, which safeguards against unreasonable searches. However, the examination of electrical records was not considered a violation since the information collected from it lacked sufficient verification.<sup>77</sup> It also observed that the private medical history of an individual would fall within the core of personal information protected by Section 8 of the Charter. This would include details about their medical conditions, treatments, and sensitive personal choices related to their health. Also suggests that such information, which discloses intimate aspects of a person's life, should be safeguarded and controlled by the individual, without indiscriminate access by the state.<sup>78</sup>

In a case where a thermal imaging search was conducted, the Court concluded that there was no violation of Section 8 of the Charter because the thermal imaging did not reveal any significant personal evidence or aspects of the individual's private life. The Court also emphasized the importance of differentiating between personal privacy, territorial privacy, and informational privacy when determining if Section 8 of the Charter has been infringed.<sup>79</sup> Let's consider a simple example to illustrate the distinction between these types of privacy. Imagine a person living in a house.

- ♦ **Personal Privacy:** Personal privacy refers to intimate aspects of an individual's private life, such as their personal conversations, daily routines,

<sup>74</sup> Ibid.

<sup>75</sup> Ibid.

<sup>76</sup> R v. *Plant*, [1993] 3 S.C.R. 281

<sup>77</sup> Ibid.

<sup>78</sup> R v. *Walter Tessling*, [2004] 3 S.C.R. 432

<sup>79</sup> [1990] 1 S.C.R. 30

or private activities conducted within the confines of their home. For instance, personal privacy would encompass conversations between family members in the living room, personal grooming activities in the bathroom, or moments of relaxation in the privacy of one's bedroom.

- ♦ **Territorial Privacy:** Territorial privacy relates to the physical boundaries and the protection of one's property. It includes the right to control access to one's home and property. For example, an individual has territorial privacy when they can prevent unauthorized entry into their house or secure their backyard from unwanted intrusions.
- ♦ **Informational Privacy:** Informational privacy refers to the protection of personal information, such as sensitive data, records, or details that could be used to identify or expose aspects of an individual's life. It covers confidentiality and control over personal data, such as medical records, financial information, or private correspondence. For instance, informational privacy would involve safeguarding one's email communications, bank statements, or medical history from unauthorized access or disclosure.

The Court's statement highlights the importance of considering these distinct aspects of privacy when evaluating if a violation of Section 8 of the Charter has occurred. In the case involving thermal imaging, the Court concluded that since the thermal imaging did not reveal any personal evidence or delve into the individual's private life, there was no infringement of Section 8.

In *R v Duarte*<sup>80</sup>, Duarte was being investigated by the police for narcotics offences. An undercover cop set up a meeting with Duarte at a rented room where the cops had hidden a video camera. Duarte was convicted based on video evidence. Duarte appealed on the ground that he needed to give consent to be recorded. The issue was elevated that, Did the use of the video camera violate Duarte's rational expectation of privacy? The court held that, yes, a secret recording of private communications constitutes unreasonable search & seizure and could be accepted if the state shows its interests, based on reasonable & feasible grounds, are greater than an individual.

In *R v Spencer*<sup>81</sup>, Canadian Supreme Court reiterated the considerations to be examined in determining a reasonable consideration of privacy, including, “(a) the subject matter of the suspected search; (b) the claimant's interest in the subject material; (c) the

---

<sup>80</sup> 2014 SCC 43

<sup>81</sup> Ibid.

*claimant's expectation of privacy in the subject matter; and (d) whether this personal expectation of privacy was objectively reasonable, having regard to the totality of the situations?*

The Court statement also acknowledges that informational privacy is multifaceted and includes these three interconnected aspects: privacy as secrecy (protection of personal information), privacy as control (authority over personal data), and privacy as autonomy (freedom to live and make choices without excessive intrusion).<sup>82</sup>Talking about the other developed nations like Sweden<sup>83</sup>, Netherlands<sup>84</sup> have their own Constitution which expressly stated that the right to privacy is their fundamental right whereas,in the Constitution of Denmark<sup>85</sup>Article 72 provides for secrecy without mentioning the expression of privacy.

One area where the right to privacy in Canada is lacking pertains to the use of warrantless searches conducted by border officials. In accordance with Canadian legislation, border officials possess the authority to conduct searches on individuals entering or leaving the country without obtaining a warrant. This grants them the ability to search electronic devices, such as cellphones, laptops, and tablets, without any requirement of suspicion or indication of wrongdoing.

This particular aspect has raised significant concerns among privacy advocates due to the fact that electronic devices often contain sensitive and personal information, including emails, social media accounts, and financial records. The acquisition and examination of this information can divulge extensive details about an individual's private life, all without the presence of any legal oversight or scrutiny.The legal framework governing warrantless searches conducted by border officials in Canada is a complex issue. The Canadian Charter of Rights and Freedoms generally upholds the right to privacy; however, this right is not absolute. Section 1 of the Charter permits reasonable limits on individual rights if they are deemed justifiable within a free and democratic society.

The Supreme Court of Canada has addressed the matter of warrantless searches by border officials in various cases. In the case of *R. v Simmons*<sup>86</sup>, the Court recognized that border officials possess broad search powers and that searches can be conducted without a warrant if they are performed for the purpose of ensuring

---

<sup>82</sup> The Constitution of Sweden, Article 6.

<sup>83</sup> The Constitution of Netherland, Articles 10, 13.

<sup>84</sup> The Constitution of Kingdom of Denmark, Article 72.

<sup>85</sup> [2008] UKHL 3

<sup>86</sup> [2017] SCC 34.

border security. Nonetheless, the Court acknowledged that warrantless searches can encroach upon an individual's right to privacy, and such searches must be reasonable given the specific circumstances.

In more recent cases, the Court has acknowledged the significant privacy interests involved in relation to electronic devices. In the case of *R. v Canfield*<sup>87</sup>, the Court ruled that border officials must have a reasonable suspicion of wrongdoing before conducting searches on electronic devices. In *R. v Vautour*<sup>88</sup>, the Court determined that border officials must confine their search to the information that is pertinent to the objectives of their search. Despite these legal decisions, the legal framework governing warrantless searches conducted by border officials in Canada continues to present a gap in the protection of the right to privacy.

The utilization of warrantless searches conducted by border officials in Canada represents a notable deficiency in safeguarding the right to privacy. Although the Canadian Supreme Court acknowledges the significance of privacy interests associated with electronic devices, the legal framework pertaining to warrantless searches by border officials remains ambiguous. Given the continuous advancement of technology, it is imperative that the legal framework is clarified and revised to guarantee sufficient protection of the right to privacy.

## B. Developing Countries

### South Africa

South Africa, as a developing country, explicitly recognizes the right to privacy as a justifiable right under Section 14 of its Constitution.<sup>89</sup> This provision replaces Section 13 of the interim Constitution of the Republic of South Africa Act 200 of 1993, which had a similar content.<sup>90</sup> The Constitution of the Republic of South Africa, 1996 also specifically acknowledges the right to human dignity.<sup>91</sup>

In South Africa, the Constitution holds paramountcy as the supreme law of the land<sup>92</sup> and the state is obligated to respect, protect, promote, and fulfil the rights enshrined in the Bill of Rights,<sup>93</sup> which apply to both state and non-state actors<sup>94</sup>. Rights can only be limited by other laws if such limitations are reasonable, justifiable, and serve a legitimate societal purpose.<sup>95</sup> Additionally, various laws impose obligations

<sup>87</sup> [2013] 3 SCR 657.

<sup>88</sup> The Constitution of the Republic of South Africa, s 14.

<sup>89</sup> Id., Section 13.

<sup>90</sup> Id., s 10.

<sup>91</sup> The Constitution of the Republic of South Africa, 1996, s 2.

<sup>92</sup> Id., Section 7(2).

<sup>93</sup> Id., Section 8.

<sup>94</sup> Id., Section 36.

<sup>95</sup> The National Health Act 61 of 2003

on the state and other entities to safeguard private information collected from the public, including the NHA<sup>96</sup>; NCA<sup>97</sup>; CPA<sup>98</sup>; ECT<sup>99</sup>; and PAI<sup>100</sup>.

In *National Media Ltd. v Jooste*<sup>101</sup>, the Court well-defined privacy in the widest of terms, including “the ability to govern the purpose of private facts.” In *Bernstein v Bester & Others*,<sup>102</sup> the Court concluded that the “Right to privacy is recognized in the truly personal dominion, but as a person moves into public relations and activities such as commercial and social collaboration, the scope of personal space curtail accordingly.” The inclination in *Bernstein*<sup>103</sup> was sustained in *Investigating Directorate, Serious Offences v Hyundai Motor Distributors Ltd.*<sup>104</sup>, in which the court observed that “man as a rational being desire to do many things but in civil society his desires to be control, regulated and reconcile with the similar desire by the other individual.” The court however stressed that “there must be a balance between the interests of the individual and that of the state, a task that lies at the heart of the inquiry into the constraint of rights.”

In a case concerning anti-sodomy legislation, the Constitutional Court rendered a ruling stating that the criminalization of sexual intimacy between gay men violated the right to equality by unjustly discriminating against them on the basis of their sexual orientation. This discrimination was deemed impermissible since the Constitution explicitly includes sexual orientation as a protected ground against discrimination.<sup>105</sup> Furthermore, in a case pertaining to same-sex marriages, the court emphasized the interconnectedness of privacy, dignity, and equality.<sup>106</sup> It highlighted that these principles extend beyond the mere concept of personal space, encompassing the right of gay and lesbian couples to live together without interference from the state. The court noted that the claimants in the case were not merely seeking the right to be left alone, but rather the right to be recognized as equals and to have their dignity upheld under the law.<sup>107</sup>

---

<sup>96</sup> The National Credit Act 34 of 2005

<sup>97</sup> The Consumer Protection Act 68 of 2008

<sup>98</sup> The Electronic Communication and Transactions Act 25 2002

<sup>99</sup> The Promotion of Access to Information Act 2000

<sup>100</sup> 1996 (3) SA 262 (SCA)

<sup>101</sup> 1996 (2) SA 751 (CC)

<sup>102</sup> Ibid.

<sup>103</sup> 2001 (1) SA 545 (CC)

<sup>104</sup> *National Coalition for Gay and Lesbian Equality v Minister of Justice*, 1999 (1) SA (CC)

<sup>105</sup> *Minister of Home Affairs and Another v Fourie and Another*, (2005) ZACC 19

<sup>106</sup> Ibid.

<sup>107</sup> 2007 (5) SA 6 (CC)

In *NM & Others v Smith & Others*<sup>108</sup>, the court determined that the author and publisher were responsible for violating and infringing upon the right to privacy of several women by disclosing their HIV status in a book. As a result, they were found liable and ordered to pay damages to the victims. Critically analyzing, it highlights the court's recognition of the importance of the right to privacy and its application in protecting sensitive personal information, such as an individual's HIV status. By disclosing this private information without consent, the author and publisher breached the privacy rights of the women involved.

The right to privacy is a fundamental and protected human right under both international and national legal frameworks. In South Africa, the Constitution of the Republic of South Africa safeguards the right to privacy in Section 14. Although South Africa has established a robust legal framework for the protection of privacy, certain gaps persist. One such gap pertains to the acquisition and utilization of personal data by governmental entities. Government agencies are amassing extensive personal data, encompassing names, addresses, financial particulars, and even biometric information like fingerprints and facial recognition data. Often, this data is collected without the knowledge or consent of the individuals involved and is subsequently employed for various purposes, including law enforcement and national security. This situation has aroused significant concerns among privacy advocates due to the potential ramifications for individual's privacy and security resulting from the collection and utilization of personal data. For instance, personal data can be exploited for surveillance, profiling, and discriminatory practices.

The legal framework governing the collection and use of personal data by government agencies in South Africa is delineated by several statutes, including the Protection of Personal Information Act (POPIA), the Regulation of Interception of Communications and Provision of Communication-Related Information Act (RICA), and the Intelligence Services Oversight Act (ISOA). Under these laws, government agencies are obligated to obtain individual's consent before collecting and utilizing their personal data. Additionally, they must take reasonable measures to ensure the accuracy and currency of the collected data while safeguarding it against loss, damage, or unauthorized access.

Despite the existence of these regulations, there are still deficiencies in safeguarding the right to privacy. Notably, the laws provide broad exemptions that permit government agencies to collect and utilize personal data without the knowledge or consent of the affected individuals, particularly for national security

---

<sup>108</sup> [2004] ZACC 1.

purposes. Consequently, individuals may remain unaware of the collection of their personal data or how it is being utilized.

In the case of Minister of Safety and Security and Others v Hamilton and Others<sup>109</sup>, the Constitutional Court of South Africa addressed the issue of the collection and use of personal data by government agencies. The Court emphasized that such practices must align with the Constitution and the law, and any limitation on the right to privacy must meet the criteria of reasonableness and justifiability in an open and democratic society. To understand this case law, let's consider an example: Suppose there is a government agency responsible for national security that wishes to collect and analyze personal data from individuals for surveillance purposes. They decide to deploy a surveillance program that involves monitoring phone calls, emails, and internet activities of individuals without their knowledge or consent. This program aims to identify potential threats to national security. In this scenario, the Constitutional Court's decision in the case of Minister of Safety and Security and Others v Hamilton and Others<sup>110</sup> comes into play. The Court would examine whether the collection and use of personal data by the government agency comply with the Constitution and the relevant laws.

The Court would assess whether the surveillance program constitutes a limitation on the right to privacy. It would consider whether the limitation is reasonable and justifiable in an open and democratic society. Factors such as the nature of the surveillance, its necessity, effectiveness, and potential impact on individuals' privacy rights would be evaluated. If the Court determines that the surveillance program disproportionately infringes on individuals' right to privacy without sufficient justification, it may declare it unconstitutional and order appropriate remedies. Conversely, if the Court finds that the program meets the requirements of reasonableness and justifiability, it may uphold its legality. Overall, this case law emphasizes the importance of balancing the need for government agencies to collect and use personal data for legitimate purposes with the protection of an individual's right to privacy, ensuring that any limitation on privacy rights is reasonable and justified in a democratic society.

In another case, the *Right2Know Campaign v Minister of State Security and Others*<sup>111</sup>, the court found certain aspects of RICA to be in violation of the right to privacy, as enshrined in the Constitution or other relevant legal principles. The

<sup>109</sup> Ibid.

<sup>110</sup> [2014] ZAGPJHC 343.

<sup>111</sup> Supra n. 4

court likely concluded that the provisions of RICA did not adequately protect individuals' privacy rights when it came to the interception of their communications. This means that the legislation in question allowed for the interception of communications in a manner that went beyond what was considered reasonable and justifiable in a democratic society. The court's ruling highlights the importance of striking a balance between the need for state security and the protection of an individual's right to privacy. It emphasizes the requirement for adequate safeguards and procedures to be in place to ensure that the interception of communications is done in a manner that respects and upholds an individual's privacy rights.

The absence of adequate safeguards in the collection and utilization of personal data by government agencies in South Africa creates a substantial loophole in safeguarding the right to privacy. Despite the existence of legal regulations, there remain deficiencies in protecting the privacy and security of individuals. It is imperative to enhance the legal framework and establish mechanisms for holding government agencies accountable for their acquisition and utilization of personal data. This is crucial to ensure the effective protection of the right to privacy.

### **India**

The right to privacy has been seen as an implied basic right under the Indian Constitution. The mounting defilement of this right stimulated the Indian Judiciary to take an active role in defending it. The right to privacy as an inalienable right was severally discussed in the constituent assembly debates. But to avoid the concept of due process of law and to avoid disturbance in the law and order, Privacy on searches and seizures was avoided and hence in totality, privacy as a fundamental right was rejected. This was followed after referring to U.S. Constitution for the concept of Privacy. In the U.S., the concept of privacy has not been mentioned explicitly in the Constitution, but certain provisions such as the First, fourth, fifth, ninth and Fourteenth Amendment explicitly mentions about right to privacy especially the fourth amendment which prohibits unreasonable searches and seizures.<sup>112</sup> Hence, the U.S. legislature along with Judiciary played an important role in the development of a right to privacy going beyond the strict interpretation of the U.S. Constitution.

In India, the right to privacy was debated for the first time in 1954 by the Hon'ble Supreme Court in the matter of *M.P Sharma v Satish Chandra*<sup>113</sup> where the case of validity of search and seizures was put before the Court. The court

---

<sup>112</sup> 1954 SCR 1077

<sup>113</sup> AIR 1963 SC 1295

determined that since Indian Constitution does not have any such amendment on the lines of the Fourth U.S Constitutional amendment, the right to privacy cannot be questioned. But later in 1962, in the case of *Kharak Singh v State of Uttar Pradesh*<sup>114</sup>, the number of police acts based on the Police regulation act was challenged in which the question of the validity of domiciliary visits<sup>115</sup> was challenged. In this case, Kharak Singh, who was once convicted in a criminal case, was kept under surveillance by the police by means of domiciliary night visits that caused mental stress and problem to him and his family. The Supreme Court gave importance to order and peace in the society and hence held the validity of regulations as privacy is not guarded by the Constitution and hence Article 21 Right to life and Personal liberty could not be brought into application<sup>116</sup>. Had a serious approach been taken by the Supreme Court regarding the necessity of this natural right, the struggle for this right would not have been so long. After these two landmark judgements, the idea of privacy remained unchallenged for several years.

Later after a few years, the privacy concept was again challenged in the case of *Govind v State of Madhya Pradesh*<sup>117</sup>, in which the court accepted privacy as secretion from Article 19(a), (d) and Article 21 but it being not an absolute right, privacy can be controlled based on gripping public interest. Moreover, the right to privacy was regarded as a right to deal with persons and not places<sup>118</sup>. The concept of the Right to privacy was sincerely expanded in the case of *Smt. Maneka Gandhi v Union of India*<sup>119</sup> in the year 1978 in which 7 Judge bench introduced a triple test to identify interference with the right to life and personal liberty. The first was the prescription of a specific procedure that must pass the test of one or more of the basic rights bestowed under Article 19 that are relevant in the current scenario, and finally, that method must pass the test of Article 14.

Further, in the case of *R. Rajgopal v State of Tamil Nadu*<sup>120</sup>, it was held by Justice B.P Jeevan Reddy observed that intrusion in one's life, family, procreation, motherhood, education etc. would amount to the right to privacy as implicit in the right to life and personal liberty. In view of the above verdicts, it can be evident that though the right to privacy is not expressly stated as a fundamental right in the Indian Constitution, the same right has expanded significantly in India, and privacy is now considered as immediately flowing from the right to life and personal liberty.

---

<sup>114</sup> House visit by Police official at night, making sure that suspect is in house or gone out.

<sup>115</sup> Supra n. 35

<sup>116</sup> 6 AIR 1975 SC 1379

<sup>117</sup> Ibid.

<sup>118</sup> AIR 1978 SC 597

<sup>119</sup> AIR 1995 SC 264

<sup>120</sup> AIR 1997 SC 568

Moreover, the ambit of privacy was widened in the case of the *People's Union for Civil Liberties v. Union of India*<sup>121</sup> the scope of privacy was expanded to encompass telephone tapping conducted by the government under the Telegraph Act. The court determined that such interception violated Article 21 of the Constitution, which protects the right to life and personal liberty. This decision recognized that privacy is an inherent aspect of an individual's fundamental rights. Furthermore, in the case of *Ram Jethmalani v. Union of India*<sup>122</sup>, the court emphasized that the right to privacy is an essential component of the right to life. Although the Constitution does not explicitly mention the right to privacy, it can be derived from the provisions of Article 21. The court acknowledged that telephonic conversations fall within the realm of privacy, and any unauthorized tapping or interception of such confidential information constitutes a violation of the right to privacy. According to these rulings, the right to privacy is considered fundamental and protected under the Constitution. It is intricately linked to the right to life and personal liberty. Any infringement upon this right, including the tapping of telephonic communications, can only be justified if it follows the procedure established by the law.

Recently, in *Justice K. S. Puttaswamy (retd.) v. Union of India*<sup>123</sup>, a nine-judge Constitution Bench of the Supreme Court ruled that the right to privacy is an inherent part of life and liberty under Article 21. The issue particularly brought before the court was to decide upon the validity of biometric identity based upon the Aadhar Scheme where the nine-judge bench expanded the issue by deciding upon privacy as a fundamental right or not. The arguments given by the attorney general against the right to privacy were with reference to the intent of constitution-makers and accepting the right to privacy would amount to rewriting the constitution. But the nine Judge Bench led by Retd. Chief Justice J.S Khehar, upheld the right to privacy and extended the date for deciding upon the validity of the Aadhar scheme. Aadhar, the largest biometric system in the world, was introduced in India for helping people to avail benefits of certain government schemes such as availing Rations etc., but due to its security breaches, the Aadhar had become the most unsafe scheme containing sensitive data such as fingerprints, retina scan and other personal information. Moreover, the Information Technology Act, of 2000 is the only source of protection of data in India and hence, privacy had become more important in the Indian Context to avoid data breaches. Later deciding upon the validity of Aadhar concerning Privacy, the Supreme Court laid down a proportionality test to determine whether a law is reasonable or not. For this, four aspects namely,

<sup>121</sup> (2011) 8 SCC 1

<sup>122</sup> AIR 2015 SC 3081

<sup>123</sup> 410 U.S. 113 (1973)

Legitimate goal, Rational Connection, Necessity and balancing were laid down and applied to check the validity of the Aadhar Case. Observing and analysing all four aspects for the reasonability of the Aadhar scheme, the Hon'ble Court only held the validity of linking Aadhar with the Pan Card but denied the proportionality of linking Aadhar with bank accounts and mobile numbers. Further, the right to privacy does not only indicate data privacy but also includes privacy from social intrusion.

Apart from the various judicial assertions on the right to privacy in India, under the guidance of Justice A P Shah, a Committee of Experts was formed to study privacy legislation & its recommended the following suggestion on the draft Bill on Privacy.

- a) "Enactment of new and comprehensive laws to protect privacy in the private & public spheres.
- b) Privacy commissioners shall be appointed at both Centre as well as the state level.
- c) Creation of Self-Regulating Organisations by the industry for enforcing the right to privacy.
- d) Pen down Nine principles of privacy such as Notice, Choice & consent, Collection limitation, Purpose Limitation, Access & Correction, Disclosure of information, Security, Openness, and Accountability to be followed by the data controller.
- e) Also recommended limitation on the right to privacy such as national security, public order & public interest, tackling criminal offences, protection of the rights of freedom of others."

The development of the Right to privacy in India took a long time to shape its identity whereas it was developed in the U.S. much earlier. After the first case of the right to privacy in the U.S, another case that was put before the U.S Supreme Court was regarding the constitutionality of Texas abortion law in the case of *Roe v. Wade*<sup>124</sup> in which the Court held the right of privacy emerging from fourteenth U.S constitutional amendment which deals with the right to personal liberty and restriction against state action. Whereas it took almost 60 years in India after two landmark judgments, to interpret the concept of privacy as a part of the right to personal liberty of a person under Art. 21.

The absence of comprehensive data protection laws in India constitutes a significant gap in the right to privacy. This gap arises from the lack of a dedicated law specifically addressing data protection and the inadequate protection provided

---

<sup>124</sup> The Constitution of Russian Federation, art 23.

by existing laws, such as the Information Technology Act, of 2000, and its accompanying rules. These laws fail to adequately safeguard personal data, which raises concerns among privacy advocates.

The collection and use of personal data can have profound implications for an individual's privacy and security. Given the increasing instances of data breaches and privacy violations, including notable cases like the Cambridge Analytica scandal, there is a pressing need for a robust data protection regime in India. The lack of comprehensive data protection laws not only leaves individuals vulnerable to privacy infringements but also hampers their ability to exercise control over their personal information. It also poses challenges in holding accountable those responsible for mishandling or misusing personal data. To address this gap, India should prioritize the enactment of a comprehensive data protection law that aligns with international best practices and ensures the protection of individual's privacy rights. Such a law would establish clear guidelines for data collection, processing, storage, and sharing, along with robust mechanisms for enforcement and accountability. By implementing an effective data protection regime, India can strengthen the right to privacy, enhance individuals' control over their personal data, and foster trust in the digital ecosystem. Furthermore, other developing countries like Russian Federation<sup>125</sup>, Brazil<sup>126</sup>, and Bulgaria<sup>127</sup> specifically embodied the right to privacy under their constitutions.

### **C. Least Developed Countries**

#### **Nepal**

Following the promulgation of the Nepal Constitution in 2015, the country's legal system was transformed into a federal structure. The changes were widely considered to be the foundations of the modern legal system in the country. The implementation of the Individual Privacy Act 2018 was one of the most significant improvements since it gave reality to the right to privacy enshrined in the Nepal Constitution<sup>128</sup>.

---

<sup>125</sup> The Constitution of Brazil, Article 5, X, XI, XII, XXXVIII.

<sup>126</sup> The Constitution of Bulgaria, Articles 32, 33.

<sup>127</sup> The Constitution of Nepal, Article 28.

<sup>128</sup> NKP 2074, D.N. 9740, p 25

The Supreme Court of Nepal in *Baburam Aryal v GON*<sup>129</sup> has held that the right to privacy is a fundamental right that can be infringed upon by third parties. As such, it has been observed that certain activities related to a person's residence, body, property, and communications violate this right. In a case involving the Prime Minister's Office and the Council of Ministers of Nepal, the Supreme Court ruled that the right to privacy is of the utmost importance. An exception to this right exists only when prior consent from the person concerned has been obtained.<sup>130</sup>

The right to privacy in Nepal, despite being constitutionally guaranteed, faces significant gaps in its protection. One such gap pertains to the absence of comprehensive data protection laws in the country. Nepal lacks a dedicated data protection law, and the existing laws, such as the Electronic Transactions Act of 2008 and its rules, are insufficient in safeguarding personal data. This dearth of robust data protection regulations is a matter of concern for privacy advocates, as the collection and utilization of personal data can have profound implications for individuals' privacy and security. Nepal has witnessed various instances of data breaches, including the notable Nepal Telecom data breach, underscoring the urgent need for a more comprehensive data protection framework.

Another area of concern is the widespread use of CCTV cameras in Nepal, employed by both public and private entities for security purposes. However, the use of CCTV cameras raises apprehensions regarding the potential infringement on the right to privacy. Instances of unauthorized surveillance and privacy invasion through CCTV cameras have been reported. Moreover, the absence of specific regulations governing the use of CCTV cameras exacerbates the situation. Nepal lacks a dedicated law that governs the usage of CCTV cameras, resulting in potential misuse and abuse of this technology. The legal framework governing the right to privacy in Nepal comprises several laws, including the Constitution of Nepal, the Electronic Transactions Act of 2008, and the Civil Code of 2017. However, the current legal provisions fall short of providing comprehensive protection for privacy rights in the digital age, necessitating the development of more robust and tailored legislation.

In the case of *Nayan Raj Pandey v Government of Nepal and Others*, the Supreme Court of Nepal recognized the right to privacy as a fundamental right protected under the Constitution of Nepal. This landmark decision established the importance of safeguarding individual privacy from unwarranted intrusion by the state or other entities. The court further emphasized that any infringement on the right to privacy must be justified by a compelling state interest. This means that the government or any other entity seeking to infringe upon an individual's privacy must demonstrate a legitimate and pressing reason for doing so. Additionally, the

<sup>129</sup> *Sapana Pradhan Malla v. Office of the Prime Minister and Council of Ministers et. al.*, NKP 2064, D.N. 7880, P 1208

court held that the infringement must be proportionate to the objective being pursued, ensuring that the extent of intrusion does not exceed what is necessary to achieve the intended purpose.

To illustrate this, let's consider an example. Suppose there is a government initiative to install surveillance cameras in public spaces with the aim of enhancing public safety. In implementing this measure, the government would need to justify its actions by demonstrating a compelling state interest, such as reducing crime rates or protecting citizens from potential threats. However, the installation and use of surveillance cameras must be proportionate to the intended objective. Excessive monitoring or indiscriminate surveillance of individuals' activities would constitute an unjustifiable infringement on their right to privacy.

In this case, the Supreme Court's ruling serves as a safeguard against potential abuses of the right to privacy. It ensures that any infringement on privacy rights must meet the criteria of compelling state interest and proportionality, striking a balance between protecting individuals' privacy and advancing legitimate societal concerns. Insufficient data protection laws and the consequences of CCTV camera usage present notable deficiencies in safeguarding the right to privacy in Nepal. Despite existing legal regulations, there are still gaps in protecting individual privacy and security. Strengthening the legal framework is crucial, including the enactment of comprehensive data protection laws, to ensure the adequate protection of the right to privacy. Additionally, the utilization of CCTV cameras should be governed by stringent regulations to safeguard the privacy and security of individuals.

## Bangladesh

Among the various fundamental rights of the people of Bangladesh, the right to privacy is one of them. There is no specific provision in the Constitution that states that the right to privacy is a fundamental right. Nevertheless, Article 43<sup>131</sup> of the Bangladesh Constitution recognized the right to privacy indirectly. In Clause (a) of Article 43 of the People's Republic of Bangladesh's Constitution, every citizen has the right to be secure in his home against entry, search, and seizure. It is similar to the provisions of the US Constitution<sup>132</sup>, the Constitution of Luxembourg<sup>133</sup>, the Constitution of Moldova<sup>134</sup> and the Constitution of Belgium<sup>135</sup>.

---

<sup>130</sup> The Constitution of the People's Republic of Bangladesh 1972, Article 43.

<sup>131</sup> Fourth Amendment of the US Constitution.

<sup>132</sup> The Constitution of Luxembourg, Article 15.

<sup>133</sup> The Constitution of Moldova, Article 29.

<sup>134</sup> The Constitution of Belgium, Article 16.

<sup>135</sup> The Constitution of the People's Republic of Bangladesh 1972, Article 43(a).

In Bangladesh, the right to privacy of letters, telegrams, and other forms of communication is a fundamental right guaranteed by the country's constitution.<sup>136</sup> This right is also applicable to the use of telephone calls and other forms of communication. Similar provisions are also found in the constitutions of Ethiopia<sup>137</sup>, Germany<sup>138</sup>, Guinea-Bissau<sup>139</sup>, Kuwait<sup>140</sup>, Gabon<sup>141</sup> and Egypt<sup>142</sup>. The distinction between the right to privacy of communication and private life was made clear in these constitutions. For instance, in Bangladesh, the right to privacy is guaranteed as a fundamental right.

The right to privacy is a fundamental human right that is protected under international human rights law and the Constitution of Bangladesh. Article 43 of the Constitution of Bangladesh provides for the protection of the right to privacy. However, despite the constitutional guarantee, there are gaps in the protection of the right to privacy in Bangladesh. The significant gap in the protection of the right to privacy in Bangladesh is the lack of comprehensive data protection laws. While there are some laws that provide for the protection of personal data, they are limited in scope and do not provide adequate protection for individuals' privacy.

The current laws that address data protection in Bangladesh are the Bangladesh Telecommunication Regulatory Act 2001, the Right to Information Act 2009, and the Digital Security Act 2018. However, these laws do not provide comprehensive protection for personal data and fail to address emerging privacy concerns, such as the collection, storage, and use of personal data by social media platforms. The use of surveillance technologies in Bangladesh, including CCTV cameras and electronic surveillance, has raised concerns about the impact on the right to privacy. The government has expanded its surveillance capabilities in recent years, including the installation of CCTV cameras in public spaces, the monitoring of social media, and the use of facial recognition technology.

The lack of regulations surrounding the use of surveillance technologies has become a significant concern for privacy advocates, as the use of these technologies can have a chilling effect on freedom of expression and association. There have also been reports of abuses of surveillance technologies, such as the harassment and intimidation of political dissidents and journalists. The legal framework surrounding the right to privacy in Bangladesh is governed by several

---

<sup>136</sup> The Constitution of Ethiopia, Article 26(2).

<sup>137</sup> The Constitution of Germany, Article 10(1).

<sup>138</sup> The Constitution of Guinea-Bissau, Article 48(1).

<sup>139</sup> The Constitution of Kuwait, Article 39.

<sup>140</sup> The Constitution of Gabon, Article 1(5).

<sup>141</sup> The Constitution of the Arab Republic of Egypt, Article 57.

<sup>142</sup> The Constitution of Chad, Article 42.

laws, including the Constitution of Bangladesh, the Bangladesh Telecommunication Regulatory Act 2001, the Right to Information Act 2009, and the Digital Security Act 2018. Furthermore, other least-developed countries like Chad<sup>143</sup>, Ethiopia<sup>144</sup>, and Rwanda protect the privacy of a person and family under the Constitution of the Republic of Rwanda<sup>145</sup>, Sudan<sup>146</sup> also expressly penned down the right to privacy under their Constitution.

### **Conclusion**

To conclude, the influence and diversity of cultures, religious, economic, as well as development-political factors make it difficult to compare privacy perceptions of developed and least developed countries. The respective comparison countries are in different starting positions. Under the influence of these factors and while complying with municipal demands, each of the observed countries tries to attain its objectives through a functional approach to privacy. We can observe, however, that there is a divergence in the diversity and distribution of digital technologies between developed and developing nations and that this involves a different approach to privacy. Since these technologies are readily available and widely used, they are often used for official purposes by the respective states, which is why they have been mandated to be used by citizens.

The choice of whether digital technologies are used, and privacy becomes more vulnerable is only theoretically available to low-income persons since the waiver of the ‘reward of information provision’ is out of the question. This corroborates the economic influence on privacy already mentioned in the above quote from a participant from South Asia. The described measures of the examined countries are based almost exclusively on external motivation or the fear of the consequences of missing measures. In many countries, the fulfilment of information security requirements for third countries, as required by many data protection laws of industrialized countries and confederations, has been an important driver in the efforts to develop their data protection laws. The granting of a right to privacy was often only secondary, as evidenced, for example, by the lack of rules on data subject’s rights.



---

<sup>143</sup> The Constitution of the Federal Democratic Republic of Ethiopia, Article 26(1)(2)(3).

<sup>144</sup> The Constitution of the Republic of Rwanda, Article 23.

<sup>145</sup> The Constitution of the Republic of the Sudan, Article 55.